RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: SAT-R03

AI-Enabled Cybercrime: Separating Hype from Reality

MODERATOR: **Leah Walker**
Lab Director, Berkeley Risk and Security Lab

PANELISTS: **Derek Manky**
Chief Security Strategist & VP Global Threat Intelligence, Fortinet

Helena Yixin Huang
Associate Research Fellow, S. Rajaratnam School of International Studies, Nanyang Technological University

Dr. Gil Baram
Non-resident Research Scholar, University of California, Berkeley

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

#RSAC

Many Voices.
One Community.

MODERATOR:

Leah Walker

Lab Director, Berkeley Risk and Security Lab

PANELISTS:

Derek Manky

Chief Security Strategist & VP Global Threat Intelligence, Fortinet

Helena Yixin Huang

Associate Research Fellow, S. Rajaratnam School of International Studies, Nanyang Technological University

Dr. Gil Baram

Non-resident Research Scholar, University of California, Berkeley

Debunking Myths

- Common misconceptions about AI-enabled cyber threats
- Myth: “AI will autonomously hack systems without human involvement.”
  - Reality: AI is an accelerator but still requires human cybercriminals.
  - Example: AI doesn’t “think” like a hacker—it assists with phishing, automation, and evasion.
- Myth: “AI attacks are unstoppable.”
  - Reality: Defensive AI is advancing alongside offensive AI.
  - Example: AI-enabled fraud detection in banks has significantly reduced AI-generated phishing success rates.

Current State of AI-Enabled Cybercrime

- How AI is being used in cybercrime today?
- How do these AI-enhanced attacks differ from traditional cyber threats?
- What unexpected challenges have emerged in detecting and mitigating these threats?
- What existing security measures have proven effective or ineffective against AI-enabled crime?

Future Developments

- Which theoretical AI-enabled attacks are closest to becoming reality?
- How will AI-enabled cybercrime change the makeup of the cybercrime marketplace? What new services can we expect on the horizon, and what impact is that going to have to end users and potential victims of cybercrime?
- How can organizations prepare for emerging threats without overreacting to unlikely scenarios?
- What will we be discussing if we have this panel again at RSAC 2026?

Wrap Up

- AI is already enhancing cybercrime, but not in the way Hollywood portrays.
- Defenders must adapt: AI can be used defensively to counter AI-enhanced threats.

Apply What You Have Learned Today (1)

- Next week you should:
  - **Audit AI exposure**: Identify potential areas in your organization vulnerable to AI-driven cyber threats (e.g., phishing, Deepfakes, automation).
- In the first three months following this presentation you should:
  - **Enhance authentication methods** to counter AI-driven identity fraud (e.g., multi-factor authentication, biometric detection).
  - **Build awareness training for security teams**: Teach SOC analysts how AI enhances social engineering (Deepfake voice scams, AI-authored phishing).
  - **Deploy AI-based security tools:** to detect AI-powered threats (e.g., behavioral analysis for fraud detection).

Apply What You Have Learned Today (2)

- Within six months you should:
  - **Drive an implementation project** to raise employees awareness for the ways AI is enhancing cybercrime and where it could ‘meet’ them - at work and at home.
  - **Brief** your organization’s leadership team on the AI-cybercrime landscape and what it means for your organization
  - **Monitor** AI-driven cybercrime trends and collaborate with industry groups to stay ahead.

RSAC 2025 Conference

Many Voices.
One Community.

Thank You